Refine Search

Your wildcard search against 10000 terms has yielded the results below.
Your result set for the last L# is incomplete.
The probable cause is use of unlimited truncation. Revise your search strategy to use limited truncation.

Search Results -

Terms	Documents
L6 and @ad<=20001113 and (compar$ with hash$ with (number$ or value)) and (encrypt$ with content) and ((updat$ or cop$) same content)	1

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L7

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Friday, June 03, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L7	l6 and @ad<=20001113 and (compar$ with hash$ with (number$ or value)) and (encrypt$ with content) and ((updat$ or cop$) same content)	1	L7
L6	(4932054 | 5960081 | 5339091 | PCT/US98/11680 | 5898779 | 6119229 | 5010571 | 4891838 | 5664998 | 5204897 | 5159182 | 5184830 | 5103476 | 5191193 | 5113519 | 5809144 | 5138712 | 4977594 | 5872973 | 3790700 | 5247575 | 5146499 | 5023907 | 5530759 | 6226412 | 5291596 | 5125671 | 5260999 | 5774125 | 4613134 | 5356151 | 5359510 | 5050213 | 5850442 | 4378118 | 4953209 | 5393062 | 5672131 | 5498003 | 5892904 | 4658093 | 4552360 | 5047928 | 5058164 | 4529870 | 5255106 | 4961142 | 4924378 | 5704837 | 5409234 | 6009458 | 4569526 | 4937863 | 5014234 | 5872848)![PN]	54	L6
L5	('6131162'| '6591250'| '5715403')[PN]	3	L5

reviewed

Backward Refs.

L4: Entry 1 of 4 File: USPT Feb 22, 2005

DOCUMENT-IDENTIFIER: US 6859790 B1
TITLE: Data distribution system and method thereof, data processing device, data control device, and machine-readable recording medium recording distribution data

Abstract Text (1):
A contents provider stores contents data in a container in a format which can only be decoded with a key distributed from an EMD service center, and transmits the container to a service provider. The service provider adds pricing information and the like and distributes this to a user home network. The user home network pays charges to the EMD service center based on the pricing information, receives the key, and decodes the contents data. Information regarding the number of times which copying is permitted is contained in the secure container, and the number of times permitted is increased each time charges are paid, thereby enabling copying to other media and the like. It is impossible to make copies from a container simply copied, or in cases where in the number of permitted times of copies has been used up. Thus, contents data can be distributed in a format wherein copying of contents data can be controlled including the number of copies made.

Application Filing Date (1):
20001018

Brief Summary Text (7):
The copy control bits are bits representing the state whether or not the contents can be copied, and the category code are bits representing the path, of from what sort of media or what sort of network the contents were previously recorded.

Brief Summary Text (10):
For example, the CCI (Copy Control Information) and CGMS-A/D (Copy Generation Management System) being considered by the CPTWG (Copy Protection Technical Working Group) which is an operation organization of the copyright-related industry started to deal with DVD-ROM copyright protection issues, and the EMI-CCI (Encryption Mode Indicator-CCI) used with the 1394CP (Content Protection) which is a copyright protection measure for inter-equipment (home electronics) digital interfaces, but all of these end up simply changing the names of the SCMS copy control bits and continuing to use the same.

Brief Summary Text (14):
Now, rapid digitizing of broadcast networks, communication networks, and home electronics has necessitated the advent of high-level technology such as encryption technology and electronic watermarking technology, as a system to protect copyrights of digital contents. Further, the present state has reached a point which SCMS cannot deal with, even as a system to control copying.

Brief Summary Text (18):
For example, in the event that one legally purchases a packaged media and lends it to a friend, the friend is capable of making as many copies as he/she wants to, to his/her recording media. Lending the packaged media to multiple friends allows each of them to make an infinite number of copies to their recording media. Moreover, in the event that one legally purchases a packaged media and copies this to a recording medium, and distributes this to a friend, the friend can obtain the

contents for free.

Brief Summary Text (24):
Such various types of problems regarding copy control of digital contents are being pointed out from the copyrighting side, and it should be noted that each of these problems arise from the fact that the SCSM permits an infinite number of copies to be made in parallel generations.

Brief Summary Text (34):
To this end, the data distribution system according to the present invention comprises: a data distributing device which adds to desired contents data which is the object of distribution use control information containing information of the number of permitted times of use, which is the number of times that arbitrary use including either one or both of recording and playing the contents data is to be permitted and generates distribution data; and a data processing device which, based on the information of the number of permitted times of use of the contents data of the generated distribution data, detects whether or not the use of the contents data is permitted, uses the contents data in the event that use thereof is permitted, and updates the use control information so as to decrease the number of permitted times of use based on the usage.

Brief Summary Text (35):
Also, the data distribution method according to the present invention: adds to desired contents data, in a manner wherein external operation is impossible; use control information containing information of the number of permitted times of use, which is the number of times that arbitrary use of the contents data including either one or both of recording and playing the contents data is to be permitted, and generates distribution data; distributes the distribution data to a desired distribution destination; detects whether or not the use of the contents data of the distribution data is permitted, based on the use control information of the distributed distribution data, at the distribution destination; uses the contents data in the event that use thereof is permitted as the result of the detection; and updates the use control information so as to decrease the number of permitted times of use according to the usage.

Brief Summary Text (36):
Also, the data processing device according to the present invention comprises: control information extracting means for extracting, from distribution data wherein use control information containing information of the number of permitted times of arbitrary use of the contents data including either one or both of recording and playing the contents data has been added to desired contents data, information of the number of permitted times of use from the use control information; use permitting means for detecting whether or not use of the content data is permitted, based on the extracted information of the number of permitted times of use; use control means for controlling the use so as to use the contents data in the event that use thereof is permitted as the result of the detection; using means for using the contents data based on the control; and control information updating means for updating the use control information so as to decrease the number of permitted times of use, based on the usage.

Brief Summary Text (37):
Also, the data use control device according to the present invention is provided to a device which uses the contents data of distribution data wherein use control information containing information of the number of times that arbitrary use of the contents data including either one or both of recording and playing the contents data is to be permitted, is added to desired contents data to be distributed; the data use control device comprising: control information extracting means for extracting, from the distributed distribution data, information of the number of permitted times of use of the use control information; use permitting means for detecting whether or not use of the content data is permitted, based on the

extracted information of the number of permitted times of use; use control means for controlling use so as to use the contents data in the event that use thereof is permitted as the result of the detection; and control information updating means for updating the use control information so as to decrease the number of permitted times of use, based on the usage, in the event that the contents data is used.

Detailed Description Text (12):
The distribution key is sequentially validated and updated every certain period, such as once a month, and the key server 114 generates and stores several months worth of distributing keys, and transmits several months worth together to the contents provider 200, service provider 300, and user home networks 400.sub.-1 and 400.sub.-2.

Detailed Description Text (19):
The information of whether or not registration can be made indicates whether or not the contents can be used, and for example, in the event that there is a request for registration from equipment in the user home networks 400.sub.-1 and 400.sub.-2, the user registration database is searched, and depending on the recorded contents thereof, the equipment is registered or registration thereof is denied. This information of whether or not registration can be made is continuously updated, based on information such as whether there have been any unpaid bills or unauthorized processing, etc., provided from settlement firms such as banks and credit companies, the service provider 300, and so forth. Accordingly, the user administrative unit 118 denies registration of equipment having an ID which has been recorded to be registration not available, due to unpaid bills for example, and subsequently this equipment cannot use contents.

Detailed Description Text (111):
The amount of money required for one copy may be set so as to be an equal price however many copies are made, or set to decrease each time the number of copies increase, to service the customer. Also, an inverse arrangement may be taken to restrict the number of copies made. In any case, this is determined by the contents provider 200 or the service provider 300.

Detailed Description Text (117):
With the purchasing method, the user buys the contents with an amount of money equivalent to the contents from the beginning. This is a format close to the way in which contents are currently being sold. However, there is no need to permit unconditional and unlimited use of the contents, and an arrangement may be made wherein the maximum number of times of use, maximum number of times of playing, maximum number of copies, etc., may be restricted by being listed in the handling policies.

Detailed Description Text (133):
Now, in the event that the user desires to copy two generations to the parallel generations (media E/F), two of the recording tickets held are counted, and the contents are copied to the media E and F. At the same time, the user desires to copy in the serial generation direction of the media F, so one recording tickets is handed over. Consequently, the media F has one copy ticket, and the media C has used all of the tickets and has zero.

Detailed Description Text (137):
Performing copy restriction in this manner can completely restrict copies being made from rented packages which were legitimately purchased. It is appropriate that the user be allowed one copy as an already-had right, for contents of purchased packaged medial.

Detailed Description Text (167):
Then, the value obtained by passing the current value through the hash function once each time the user makes a copy is compared with the permitted number of

generations, confirmation is made regarding whether or not this has exceeded the purchased number of tickets, and if not so, the copy action is permitted.

Detailed Description Text (175):
Consequently, the number of permitted generations and the current value of the media B, D, D, and E are T(1), T(2), T(3), and T(4), and the number of recording tickets is zero, and in this state contents are copied.

Detailed Description Text (182):
Further, in FIG. 23, the contents are copied to the media E by the recording ticket of the media C.

Detailed Description Text (236):
Also, with the EMD system 1, the media A at the playing side can connect to the EMD service center at the same time as purchasing contents and purchase a necessary number of recording tickets beforehand. Accordingly, an equivalent amount is returned to the copyright holder at this point, and the media A has the right to make as many copies as the number of recording tickets purchased, so subsequent copying can be performed offline, not connected to the network. That is, perpetual communication with the EMD service center 100 is not necessary, and settlement can be made offline.

Detailed Description Text (257):
Information regarding what sorts of contents were copied to which media is stored in the storing module 473 which is secret memory within the SAM 462, in the equipment such as the communication recording/playing device 450 and the recorder 453 with SAMs installed.

US Reference Patent Number (1):
5715403

CLAIMS:

1. A data distribution system, comprising: a data distributing device which adds to desired contents data which is the object of distribution use control information containing information of the number of permitted times of use, which is the number of times that use including either one or both of recording and playing said contents data is to be permitted, and generates distribution data; and a data processing device which, based on the information of the number of permitted times of use of said contents data of said generated distribution data, detects whether or not the use of said contents data is permitted, uses said contents data in the event that use thereof is permitted, and updates said use control information so as to decrease said number of permitted times of use based on said usage; wherein said data processing device comprises a signal processing device wherein external observation and alteration of the signal processing state is impossible, and wherein said signal processing device performs detection of whether or not use of said contents data is permitted, control of use of said contents data based on said detection results, and updating of said use control information based on said use; wherein in the event of recording said contents data, said data processing device generates new distribution data by adding to said contents data said use control information containing said information of the number of permitted times of use that has been newly, and performs recording with said distribution data as a unit; and further comprising an administration device which is connected so as to be capable of communication with at least said data processing device, and which performs billing processing relating to the use of said contents data, based on information relating to use of said contents data sent from said data processing device; wherein said data processing device sends information relating to the use of said contents data to said administration device; wherein said data distributing device generates said distribution data by adding to said desired data information relating to the billing format whereby settlement can be made at said data

processing device at the time of using said contents data, as said use control information; wherein said data processing device determines the billing format for use of said contents data, based on said information relating to billing format from said use control information of said distribution data; wherein said data processing device sends information relating to the determined billing format to said administration device; and wherein said administration device performs billing processing relating to use of said contents data, based on said information relating to billing format sent from said data processing device.

2. A data distribution system, comprising: a data distributing device which adds to desired contents data which is the object of distribution use control information containing information of the number of permitted times of use, which is the number of times that use including either one or both of recording and playing said contents data is to be permitted; and generates distribution data; and a data processing device which, based on the information of the number of permitted times of use of said contents data of said generated distribution data, detects whether or not the use of said contents data is permitted, uses said contents data in the event that use thereof is permitted, and updates said use control information so as to decrease said number of permitted times of use based on said usage; wherein said data processing device comprises a signal processing device wherein external observation and alteration of the signal processing state is impossible, and wherein said signal processing device performs detection of whether or not use of said contents data is permitted, control of use of said contents data based on said detection results, and updating of said use control information based on said use; wherein in the event of recording said contents data, said data processing device generates new distribution data by adding to said contents data said use control information containing said information of the number of permitted times of use that has been newly set, and performs recording with said distribution data as a unit; and wherein said data processing device sends information relating to the number of times of use of said contents data to said administration device; and wherein said administration device performs billing processing, based on said information relating to the number of times of use of said contents data that is sent.

3. A data distribution system, comprising: a data distributing device which adds to desired contents data which is the object of distribution use control information containing information of the number of permitted times of use, which is the number of times that use including either one or both of recording and playing said contents data is to be permitted; and generates distribution data; and a data processing device which, based on the information of the number of permitted times of use of said contents data of said generated distribution data, detects whether or not the use of said contents data is permitted, uses said contents data in the event that use thereof is permitted, and updates said use control information so as to decrease said number of permitted times of use based on said usage wherein said data processing device comprises a signal processing device wherein external observation and alteration of the signal processing state is impossible, and wherein said signal processing device performs detection of whether or not use of said contents data is permitted, control of use of said contents data based on said detection results, and updating of said use control information based on said use; wherein in the event of recording said contents data, said data processing device generates new distribution data by adding to said contents data said use control information containing said information of the number of permitted times of use that has been newly, and performs recording with said distribution data as a unit; and further comprising an administration device which is connected so as to be capable of communication with at least said data processing device, and which performs billing processing relating to the use of said contents data, based on information relating to use of said contents data sent from said data processing device; wherein said data processing device sends information relating to the use of said contents data to said administration device; wherein said data distributing device generates said distribution data containing information of number of

permitted times of use represented by a hash value obtained by passing a predetermined initial value through a hash function a number of times equal to the number of times that use is permitted; and information of the essential number of times of use represented by said predetermined initial value as use control information; and wherein said data processing device restricts use of said distribution data in the event that the hash value indicating the maximum number of times of use allowed and the hash value indicating the number of times of essential use become the same.

5. A data distribution method, which: adds to desired contents data, in a manner wherein external operation is impossible, use control information containing information of the number of permitted times of use, which is the number of times that use of said contents data including either one or both of recording and playing said contents data is to be permitted, and generates distribution data; distributes said distribution data to a desired distribution destination; detects whether or not the use of said contents data of said distribution data is permitted, based on said use control information of said distributed distribution data, at said distribution destination; uses said contents data in the event that use thereof is permitted as the result of said detection; and updates said use control information so as to decrease said number of permitted times of use according to said usage; wherein detection of whether or not use of said contents data is permitted, control of use of said contents data based on said detection results, and updating of said use control information based on said use, are performed within a signal processing device regarding which external observation and alteration of the signal processing state is impossible; wherein in the event that said contents data has been used, said distribution destination sends information relating to use of said contents data to a predetermined administration device; wherein said administration device performs billing processing relating to use of said contents data, based on said generated information relating to use of said contents data; and wherein in the event of using said contents data by recording, this is performed by using as a unit; said distribution data containing said contents data and said use control information containing said information of the number of permitted times of use that has been newly set; wherein said distribution data contains information relating to the billing format for said contents data within said use control information; and wherein the billing format for use of said contents data is determined at said distribution destination, based on said information relating to the billing format of said use control information for said distribution data.

9. A data distribution method, which: adds to desired contents data, in a manner wherein external operation is impossible, use control information containing information of the number of permitted times of use, which is the number of times that use of said contents data including either one or both of recording and playing said contents data is to be permitted, and generates distribution data; distributes said distribution data to a desired distribution destination; detects whether or not the use of said contents data of said distribution data is permitted, based on said use control information of said distributed distribution data, at said distribution destination; uses said contents data in the event that use thereof is permitted as the result of said detection; and updates said use control information so as to decrease said number of permitted times of use according to said usage; wherein detection of whether or not use of said contents data is permitted, control of use of said contents data based on said detection results, and updating of said use control information based on said use, are performed within a signal processing device regarding which external observation and alteration of the signal processing state is impossible; wherein in the event that said contents data has been used, said distribution destination sends information relating to use of said contents data to a predetermined administration device; wherein said administration device performs billing processing relating to use of said contents data, based on said generated information relating to use of said contents data; and wherein in the event of using said contents data by

recording, this is performed by using as a unit; said distribution data containing said contents data and said use control information containing said information of the number of permitted times of use that has been newly set; wherein said billing is not performed for the first recording after distribution of said distribution data.

10. A data distribution method, which: adds to desired contents data, in a manner wherein external operation is impossible, use control information containing information of the number of permitted times of use, which is the number of times that use of said contents data including either one or both of recording and playing said contents data is to be permitted, and generates distribution data; distributes said distribution data to a desired distribution destination; detects whether or not the use of said contents data of said distribution data is permitted, based on said use control information of said distributed distribution data, at said distribution destination; uses said contents data in the event that use thereof is permitted as the result of said detection; and updates said use control information so as to decrease said number of permitted times of use according to said usage; wherein detection of whether or not use of said contents data is permitted, control of use of said contents data based on said detection results, and updating of said use control information based on said use, are performed within a signal processing device regarding which external observation, and alteration of the signal processing state is impossible; wherein in the event that said contents data has been used, said distribution destination sends information relating to use of said contents data to a predetermined administration device; wherein said administration device performs billing processing relating to use of said contents data, based on said generated information relating to use of said contents data; and wherein in the event of using said contents data by recording, this is performed by using as a unit; said distribution data containing said contents data and said use control information containing said information of the number of permitted times of use that has been newly set; wherein said distribution data contains information of the number of times use has been permitted and the number of times essentially already used, as said use control information, with a hash value of a hash function; and wherein detection of whether or not use of said distribution data is permitted, and updating of information indicating the number of times said distribution data has already been essentially used based on use of said distribution data, are performed by comparing information of said number of permitted times of use with information of number of times already used, at said distribution destination.

13. A data processing device, comprising: control information extracting means for extracting, from distribution data wherein use control information containing information of the number of permitted times of use of said contents data including either one or both of recording and playing said contents data has been added to desired contents data, information of the number of permitted times of use from said use control information; use permitting means for detecting whether or not use of said content data is permitted, based on said extracted information of the number of permitted times of use; use control means for controlling said use so as to use said contents data in the event that use thereof is permitted as the result of said detection; using means for using said contents data based on said control; and control information updating means for updating said use control information so as to decrease said number of permitted times of use, based on said usage; wherein said control information extracting means, said use permitting means, said use control means, and said control information updating means are configured of a signal processing device regarding which external observation and alteration of the signal processing state is impossible; wherein said use permitting means detects whether or not playing of said contents data is permitted, based on said extracted information of the number of permitted times of use; wherein said use control means controls said using means so as to play said contents data in the event that playing thereof is permitted as the result of said detection; wherein said using means plays said contents data based on said control; and wherein said control

information updating means updates said use control information based on said playing; and further comprising distribution data generating means for adding use control information containing said information of the number of permitted times of use that has been newly set to a predetermined value to said contents data, thereby generating new distribution data; wherein said use permitting means detects whether or not recording of said contents data is permitted, based on said extracted information of the number of permitted times of use; wherein said use control means controls said distribution data generating means and said using means so as to record said contents data in the event that recording thereof is permitted as the result of said detection; wherein said distribution data generating means generates new distribution data using said contents data which is the object of recording; wherein said using means records new distribution data generated based on said control; and wherein said control information updating means updates said use control information based on said new generation of distribution data and said recording.

14. A data processing device according to claim 13, wherein said distribution data contains information of number of permitted times of use by recording of said distribution data; and wherein said use permitting means detects whether or not recording of said contents data is permitted, based on said information of the number of permitted times of use by recording of said distribution data at the recording originating side; and wherein said distribution data generating means sets the number of permitted times of use by said recording of the generated distribution data, based on said information of the number of permitted times of use by recording of said distribution data at said recording originating side; and wherein said using means records new distribution data generated; and wherein said control information updating means updates said use control information based on the recording of said distribution data, and the number of permitted times of use by recording set to said recorded distribution data.

15. A data processing device according to claim 13, wherein said distribution data separately comprises information of number of permitted times of using said distribution data as original data for recording, and information of number of permitted times of using by recording for setting said distribution data as distribution data for recording as original data; and wherein said use permitting means detects whether or not recording of said contents data is permitted, based on information of the number of permitted times of use by recording of said distribution data as original data; and wherein said distribution data generating means sets the number of permitted times of use by recording of the generated distribution data, based on information of number of permitted times of using by recording for setting said distribution data as distribution data for recording as original data; and wherein said using means records said generated new distribution data; and wherein said control information updating means updates said use control information based on the recording of said distribution data, and the number of permitted times of use by said recording set to said recorded distribution data.

20. A data processing device according to claim 13, wherein, in the event of using said contents data by recording; said distribution data generating means generates said distribution data containing said use control information containing information wherein the number of permitted times of use of said contents data is set to a predetermined value smaller than the number of permitted times of use by recording of the original distribution data; said using means records said newly generated distribution data; and said control information updating means updates the information of the number of permitted times of use by recording for the original distribution data, based on recording of said new distribution data and the number of permitted times of use by recording set to said new distribution data.

21. A data processing device according to claim 16, wherein, in the event of newly increasing the number of permitted times of use of said distribution data which has

already been distributed, said communication means transmits information to said administration device for requesting a desired number of times of use of said contents data, and receives a response to said request from said administration device; and wherein in the event that said received response is such that permits said request, said control information updating means increases the number of permitted times of use of said distribution data which has already been distributed by the maximum number of times allowed.

25. A data processing device, comprising: control information extracting means for extracting, from distribution data wherein use control information containing information of the number of permitted times of use of said contents data including either one or both of recording and playing said contents data has been added to desired contents data, information of the number of permitted times of use from said use control information; use permitting means for detecting whether or not use of said content data is permitted, based on said extracted information of the number of permitted times of use; use control means for controlling said use so as to use said contents data in the event that use thereof is permitted as the result of said detection; using means for using said contents data based on said control; and control information updating means for updating said use control information so as to decrease said number of permitted times of use, based on said usage; wherein said control information extracting means, said use permitting means, said use control means, and said control information updating means are configured of a signal processing device regarding which external observation and alteration of the signal processing state is impossible; wherein said use permitting means detects whether or not playing of said contents data is permitted, based on said extracted information of the number of permitted times of use; wherein said use control means controls said using means so as to play said contents data in the event that playing thereof is permitted as the result of said detection; wherein said using means plays said contents data based on said control; and wherein said control information updating means updates said use control information based on said playing; and further comprising display means for displaying arbitrary information of said use control information of said distributed distribution data, and information based on said information.

26. A data use control device provided to a device which uses said contents data of distribution data wherein use control information containing information of the number of times that use of said contents data including either one or both of recording and playing said contents data is to be permitted, is added to desired contents data to be distributed; said data use control device comprising: control information extracting means for extracting, from said distributed distribution data, information of the number of permitted times of use of said use control information; use permitting means for detecting whether or not use of said content data is permitted, based on said extracted information of the number of permitted times of use; use control means for controlling use so as to use said contents data in the event that use thereof is permitted as the result of said detection; control information updating means for updating said use control information so as to decrease said number of permitted times of use, based on said usage, in the event that said contents data is used; and a signal processing device regarding which external observation and alteration of the signal processing state is impossible: wherein said use permitting means detects whether or not playing of said contents data is permitted, based on said extracted information of the number of permitted times of use; wherein said use control means controls said use so as to play said contents data in the event that playing thereof is permitted as the result of said detection; and wherein said control information updating means updates said use control information based on said playing; and further comprising distribution data generating means for adding use control information containing said information of the number of permitted times of use that has been newly set to a predetermined value to said contents data, thereby generating new distribution data; wherein said use permitting means detects whether or not recording of said contents data is permitted, based on said extracted information of the number of permitted times of

use; wherein said use control means controls said distribution data generating means so as to record said contents data in the event that recording thereof is permitted as the result of said detection; wherein said distribution data generating means generates said new distribution data using said contents data which is the object of recording; and wherein said control information updating means updates said use control information based on said new generation of distribution data and said recording.

27. A data use control device according to claim 26, wherein said distribution data contains information of the number of permitted times of use by recording of said distribution data; and wherein said use permitting means detects whether or not recording of said contents data is permitted, based on said information of the number of permitted times of use by recording of said distribution data at the recording originating side; and wherein said distribution data generating means sets the number of permitted times of use by recording of the generated distribution data, based on information of the number of permitted times of use by said recording of said distribution data at said recording originating side; and wherein said control information updating means updates said use control information based on the recording of said distribution data, and the number of permitted times of use by recording set to said recorded distribution data.

28. A data use control device according to claim 26, wherein said distribution data separately comprises information of number of permitted times of using said distribution data as original data for recording, and information of number of permitted times of using by recording for setting said distribution data as distribution data for recording as original data; and wherein said use permitting means detects whether or not recording of said contents data is permitted, based on information of the number of permitted times of use by recording of said distribution data as original data; and wherein said distribution data generating means sets the number of permitted times of use by recording of the generated distribution data, based on information of number of permitted times of using by recording for setting said distribution data as distribution data for recording as original data; and wherein said control information updating means updates said use control information based on the recording of said distribution data, and the number of permitted times of use by said recording set to said recorded distribution data.

33. A data use control device according to claim 26, wherein, in the event of using said contents data by recording; said distribution data generating means generates said distribution data containing said use control information containing information wherein the number of permitted times of use of contents data is set to a predetermined value smaller than the number of permitted times of use by recording of the original distribution data; and said control information updating means updates the information of the number of permitted times of use by recording for the original distribution data, based on recording of said new distribution data and the number of permitted times of use by recording set to said new distribution data.

34. A data use control device according to claim 32, wherein, in the event of newly increasing the number of permitted times of use of said distribution data which has already been distributed, said communication control means transmits information to said administration device for requesting a desired number of times of use of said contents data, and receives a response to said request from said administration device; and wherein in the event that said received response is such that permits said request, said control information updating means increases the number of permitted times of use of said distribution data which has already been distributed by the maximum number of times allowed.

Previous Doc Next Doc Go to Doc#

diff. way to obtain hash value

L4: Entry 2 of 4 File: USPT Aug 24, 2004

DOCUMENT IDENTIFIER: US 6782190 B1

TITLE: Copy protection apparatus and method

Application Filing Date (1):
19990902

Brief Summary Text (6):
Without any form of copy control, films, audio recordings and other digital content distributed on DVD disk or CD-ROM, can be easily recorded by a DVD-RAM, or other digital recorder, onto a digital data storage medium such as a recordable DVD disk, from which they can be further copied numerous times onto other DVD disks, without any degradation in the copy quality.

Brief Summary Text (10):
A further problem with the above described protection scheme is that it is inflexible, with no way of providing for a copy generation management system (CGMS), which governs the extent to which copying is permitted. For example, there is no way of providing for the contents of an original data storage medium to be copied to a back-up medium, while preventing the production of a further generation of copies from the back-up medium.

Detailed Description Text (33):
Referring again to FIG. 5, at the player 13, the reading device 14 reads the public key K and Sig.sub.K -1(S.sub.d) from the data area 3 and the disk identifier S.sub.p from the identifier area 2 of the disk 1 being played. The CCI verifier 15 calculates the hash value H(S.sub.p) and uses K to decrypt Sig.sub.K -1(S.sub.d) so as to obtain the hash value H(S.sub.d). It then compares these two hash values. If S.sub.d and S.sub.p are identical, because the disk being played is the original disk, then the hash values are also identical, then verification is successful and a signal is sent to the playback device 16 permitting playback. If S.sub.d and S.sub.p are not identical, because the disk being played is a copy of the original disk, then their hash values will be different, so that the verification process fails, which triggers a signal to the playback device 16 to prevent playback. Since the content provider is the only one to have access to the private key K.sup.-1, it is the only one that can correctly encrypt the serial number or other identifier of the original disk.

Detailed Description Text (41):
For example, the provider may decide that the content of, for example, its DVD-audio disk can never be copied. On the other hand, the provider may wish to provide its customers with the ability to make a back-up copy of the original, but not to produce further copies. The way in which these goals can be achieved is explained below using the following notation:

Detailed Description Text (42):
ID is information identifying the content provider. This can include the provider's name, the name of the content, its date of production and so on. CCF represents the copy control field, which can take the values Copy-Freely, Never-Copy, Copy-Once and No-More-Copy, as explained above. A and A' are used as convenient notation to group the provider dependent information ID and CCF together, for example, by

concatenation, such that A=ID.vertline.CCF and A'=ID.vertline.CCF', where CCF' represents a change in the value of the copy control field when recording onto a new disk. S.sub.d,S.sub.c and S.sub.p are disk identifiers printed on the read-only part of the disk. They cannot therefore be changed by the consumer. S.sub.d represents the disk identifier of the original disk, S.sub.c represents the disk identifier of the disk to which the original disk can be legitimately copied and S.sub.p represents the disk identifier of the disk being played. It will be understood that S.sub.p can take the values of S.sub.d and S.sub.c where, respectively, the original disk and a legitimate copy of the original disk, are being played. K.sub.A and K.sub.A -1 are key pairs for the digital signature of the content provider. K.sub.M and K.sub.M -1 are key pairs for the digital signature required to implement the CGMS scheme, for example to ensure that a copy is only made from the original and not from a copy of the original.

US Reference Patent Number (5):
6131162

Previous Doc Next Doc Go to Doc#

L4. Entry 3 of 4 File: USPT Jul 29, 2003

DOCUMENT-IDENTIFIER: US 6601046 B1
TITLE: Usage dependent ticket to protect copy-protected material

Application Filing Date (1):
19991203

Brief Summary Text (7):
The availability of small, inexpensive media for copying copy-protected material presents a number of potential problems as the rights of the provider of the copy-protected material are balanced with the rights of the purchaser of the copy-protected material. Because the medium is small, and intended for highly portable applications, the likelihood of the medium being lost, damaged, or misplaced is high. As such, the purchaser will. Expect to be able to reproduce the content material as often as required to replace the lost, damaged, or misplaced copies. Contrarily, because the media is inexpensive, the likelihood of an illicit mass reproduction of the content material is high, and the provider of the material will expect to be able to prevent such an illicit mass reproduction.

Brief Summary Text (3):
One method for limiting the ability to copy the content material is a "check-out/check-in" system. In this, as in other protection schemes presented herein, it is assumed that the copying and playback devices are "conforming" devices, in that they conform to the standards used to protect copy-protected material. When a copy of the material is made from a providing device to a portable medium, the conforming providing device prevents additional copies from being made until the portable medium containing the copy is returned to the providing device. This scheme has a number of drawbacks: if the portable copy is lost, damaged, or misplaced, it cannot be "returned" to the providing device, and subsequent other copies cannot be made. Such a potential "one time copy"will not be acceptable to consumers at large. Conversely, multiple copies of the content material can be made directly from the portable copy, thereby obviating the protection benefits of this scheme. Similarly, although alternative schemes that allow for N simultaneous copies of the content material onto portable media may alleviate the consumer's concern for copy-limitations, these schemes are equally susceptible to mass reproductions directly from the portable medium.

Detailed Description Text (3):
The content provider 100 receives content material, typically from a remote site, such as an Internet site, via a receiver 110, although the content provider 100 could be a conventional CD, DVD, or other medium device player that is configured to provide copies of the contents of the medium to other recording medium 200 in a copy-limited fashion. That is, the receiver 110 represents any device that provides the content material 125 that is recorded to a memory 210 of the recording medium 200, via the recorder 120. Although this invention is well suited for a solid-state memory 210, other memory storage techniques, such as the use of magnetic or optical disks, tapes, rods, and the like may also be used.

Detailed Description Text (4):
To prevent mass reproductions of the content material 125, the content provider 100 allocates a portion of a limited total-usage measure to each copy of the content

material 125 that is recorded to a recording medium 200. When the total-usage measure is completely allocated among recording media 200, the content provider 100 does not provide further recordings of the content material 125. When a recording medium 200 is returned to the content provider 100, the content provider 100 returns the portion of the total-usage measure that was allocated to the recording media 200 to the total-usage measure. That is, when each copy is "returned", the content provider de-allocates the portion that was allocated to this returned copy, thereby replenishing the total-usage measure for subsequent allocation. In this manner, the purchaser of the content material is only limited with regard to the number of co-temporal uses of copies of the protected content material.

Detailed Description Text (6):
When the "depleted" recording medium 200 is returned to the content provider 100, the total-usage measure is replenished by de-allocating the ten renderings that had been allocated to this recording medium 200. The recording medium 200 can then be reallocated a portion of the total-usage measure that is associated with the same content material 125 that it had previously received, or with new content material. Note that the total-usage measure is associated with each copy-protected content material, and can differ from, and be allocated differently from, other copy-protected content material. Because the playback device 300 or the recording medium 200 enforce the above described usage limitation, and because a conforming player 300 expects the recording medium 200 to contain this usage limitation, the illicit reproduction of the content material from the recording medium 200 will have little market value. That is, if the illicit copy includes the baseline register 230 that contains the baseline-usage parameters 145 that correspond to the allocated usage, the illicit copy will have a limited usage duration, alternatively, if it does not contain the baseline-usage parameters 145, it will not be usable on a conforming player 300. Thus, in accordance with the principles of this invention, by allocating a usage parameter to each copy of content material 125, the purchaser is provided a means for creating multiple copies of the content material 125, yet the harm caused by an illicit mass reproduction of the content material 125 is limited by an enforcement of the usage allocation. Correspondingly, a physical loss of the recording medium 200 has an acceptable effect on the purchaser, because only a portion of the allocate-able total-usage measure will be lost.

Detailed Description Text (7):
The above description illustrates the principles of this invention, but as presented, does not preclude an illicit mass reproduction. A weak link in the above description is the possibility of falsifying the aforementioned baseline-usage parameters. In a preferred embodiment of this invention, the baseline-usage parameters 145 are stored in the recording medium 200 in a verifiable form, using a security device 150. Any number of secure techniques can be employed, using techniques common in the art. In a preferred embodiment, the baseline-usage parameters 145 are either encrypted or digitally signed, or both, using a private key 151 that is associated with a "trusted source" of copy-protected material. The playback device 300 of a preferred embodiment includes a corresponding security device 350 that authenticates the source of the baseline-usage parameters 145' that are read from the recording medium 200, using a public key 351 corresponding to the private key 151 of a public-private key pair that is assigned to the "trusted source". Alternatively, a two level structure may be employed whereby a first public key embedded in the playback device 300 is used to authenticate a second key from the content provider 100. In this manner, a public key from every possible content provider need not be provided in advance. That is, the public key of the playback is used to authenticate certificates from any content provider. Each content provider will apply to the manufacturer of all playback devices for such certificates. By authenticating the source of the baseline-usage parameters 145', substituting a counterfeit baseline-usage parameter 145 onto recording medium 200 that contains an illicit copy of the content material 125 will be ineffective. On the other hand, a "blind copy" of a recording medium 200 having an authorized usage allocation associated with the content material 125 will provide for a usable

counterfeit, because the verifiable form of the baseline-usage parameters 145 will be copied as well. However, as noted above, these counterfeit copies will have minimal economic value, and thus not be a preferred target for an illicit mass reproduction, because the copied baseline-usage parameters 145 will place a limited life on the contents 125 of the memory 210 of the recording medium 200.

Detailed Description Text (9):
As an additional security measure, the recording media 200 includes a usage indicator 220 that indicates the amount of usage that the recording media 200has incurred. Preferably, the usage indicator 220 is a counter that can only be incremented, and never decremented or reset. This usage indicator will preferably contain a random value with respect to other recording media 200, so that its value cannot be predetermined. With each usage of the recording medium, the usage indicator 220 is incremented. A usage incrementer 370 is illustrated in the playback device 300, for ease of understanding, although the usage indicator 220 may be incremented by each access to-the memory 210 by a player 300, or by each insertion into a player 300, or any of a variety of explicit or implicit indications of a usage. For example, if the measure of usage is time, the recording medium 200 or the player 300 may contain a clocking system that increments the usage indicator 220 periodically. In a preferred embodiment, the content provider 100 reads the usage measure 225 from the usage indicator when the content material 125 is provided to recording medium 200. The content provider 100 uses this usage measure 225 to form thebaseline-usage parameters 145, thereby binding the baseline-usage parameters 145 to the particular recording medium 200. For example, the baseline-usage parameters 145 may contain this initial usage measure 225, and a final usage measure that is a sum of the initial usage measure 225 and the portion of total-usage that is allocated to this copy of the content material 125. The conforming playback device 300 reads (and verifies) the baseline-usage parameters 145' from the recording medium 200, via the baseline determinator 320, as well as the current value 225' of the usage indicator 220, via the usage determinator 310. In accordance with this aspect of the invention, the playback device 300 provides a rendering 361 of the content material 125' only if the current usage measure 225' is between the initial and final usage measures contained in the baseline-usage parameters 145'. By providing an increment-only usage indicator 220, illicit copies of the content material 125 cannot be produced on other recording media 200 by merely copying the baseline-usage parameters 145 from a recording medium 200 that contains a valid copy of the content material 125, because each recording medium 200 is likely to have, or can be designed to have, a statistically unique usage measure 225. That is, for example, the usage indicator can be a large counter, (e.g. 64 bits or more) that is initialized during manufacturing to a random number) and means can be provided to prevent this counter from being incremented at an excessively fast rate. A purchaser of "blank" recording medium 200 thus manufactured will not be able to use the same baseline-usage parameter 145 for each, because each medium 200 is likely to have a substantially different usage measure 225 than each other.

Detailed Description Text (10):
Other security techniques, common in the art, may also be applied. Illustrated in FIG. 1, the playback device 300 includes a ticket extractor 330 and watermark extractor 340. Generally, a watermark is a characteristic that is embedded within content material such that a removal of the watermark cannot be effected without destroying or substantially degrading the content material. As presented in copending U.S. patent application, "Copy Protection by Ticket Encryption", Ser. No. 09/333,628, filed Jun. 15, 1999 for Michael A. Epstein, incorporated by reference herein, a ticket that controls access rights to the content material can be associated with the watermark, typically via a one-way hashing function. Rules are provided for determining the validity of the ticket, based on a comparison with a hashed, or multiply hashed, value of the watermark. If the content material 125' contains a watermark but does not contain a valid ticket, the authorization device 360 prohibits its rendering 361, regardless of the validity of the above described

usage measures. In this manner, illicitly obtained content material 125 cannot be recorded onto recording media 200 that contain valid usage measures and parameters. To further prevent substitute content material 125 being illicitly recorded onto media 200 containing valid usage measures and parameters, a preferred embodiment of this invention binds the baseline-usage parameters 145 to the content material for which the portion of the total-usage measure was allocated. For example, the aforementioned ticket can be included in the baseline-usage parameters 145 that are encrypted or digitally signed before loading into the baseline-usage register 230 of the recording medium 200. An attempted counterfeit substitution of the ticket or the content material, or both, will result in a rejection by the authorization device 360 in conjunction with the security device 350. A substituted ticket will fail the aforementioned verification test based on the public key of the trusted provider, whether it matches the counterfeit content material or not, and a substituted counterfeit content material will not match a verified ticket that is associated with the original content material.

Detailed Description Text (12):
At the start of the recording, or potential recording, the current usage measure associated with the recording medium is received, at 510. Not shown in the flow diagram, if this recording medium had received a prior usage allocation from the recording device, this allocation is returned to the total-usage measure associated with the previously recorded content material. At 520, a portion of the total-usage measure associated with the content material currently being provided is allocated to this recording medium. If, at 525, an allocation is not available, because a number of other copies of this content material have been made but not yet returned, the recording process 530-560 is bypassed. The baseline-usage parameters are determined, at 530, based on the current usage measure and the allocated usage. These parameters are bound to the content material, via, for example, the aforementioned ticket that is associated with the content material, or directly to the content material, and the values and the binding are secured, at 540. The security may be an encryption of the parameters, a digital signing of the parameters, or both, and is preferably based on a private key of a public-private key pair that is associated with the provider of this content material. This secured set of parameters are recorded onto the recording medium, at 550. The public key of the public-private key pair is publicly known, and particularly known to the conforming players that are expected to read this secured information from the recording medium. At 560, the content material is recorded onto the recording medium. The process continues, at 570, wherein the recording device may issue a message confirming the completion of the recording process, or may issue a message reporting the lack of a sufficient usage allocation to provide the recording, and so on.

Detailed Description Text (13):
At the start of the playback, or rendering, process, the baseline-usage parameters are read from the recording medium, at 610 of FIG. 3. As a first test of authorization, the authenticity of the parameters is verified, at 615. As noted above, in a preferred embodiment, the parameters are encrypted or signed, or both, using a private key that is associated with a trusted provider of content material. The playback device verifies the authenticity of the parameters by, decrypting, them or by verifying the signature, or both, using the corresponding public key that is associated with the trusted provider. Other techniques for verifying the authenticity of secured items are common in the art. If the parameters are not verified as authentic, at 615, the remaining process 620-650 is bypassed. At 620, the valid period of usage is determined from the verified parameters, and at 630, the current measure of usage is read from the recording medium. If, at 635, the current measure of usage is not within the valid period of usage, the remaining process 640-650 is bypassed. At 640, the ticket and watermark associated with the content material are determined. As noted above, the ticket is preferably included in the parameters that are verified at 615. The watermark is typically determined by an extraction from the content material as it is read, using techniques common

in the art. At 645, the ticket and watermark are compared to verify that the content material is authorized to be played; if not, the rendering process at 650 is bypassed. At 650 the content material is rendered. That is, if the content material is an audio recording, audio sounds corresponding to the recording are produced; if the content material is audio-visual, audio and visual reproductions corresponding to the recording are produced; and so on. Thereafter, the process continues, at 660, wherein, for example, a "not authorized"message is rendered in response to the failed tests at 615, 635, or 645.

US Reference Patent Number (3):
5715403

Previous Doc Next Doc Go to Doc#

L4: Entry 4 of 4 File: USPT Dec 24, 2002

DOCUMENT-IDENTIFIER: US 6499105 B1
TITLE: Digital data authentication method

Abstract Text (1):
This invention provides a method for identifying a purchaser who purchased content from which an illegal copy was produced. A provider system encrypts purchased by the purchaser using a public key of a purchaser system and sends the encrypted content to the purchaser system. The purchaser system creates a digital signature of the content with the use of a private key of its own and embeds the created digital signature into the received content. When an illegal copy is found, the provider system verifies the digital signature, embedded in the illegal copy as a digital watermark, to identify the purchaser who purchased the content from which the illegal copy was produced.

Application Filing Date (1):
20000721

Brief Summary Text (22):
This technique embeds the identification of the contents purchaser into the contents in the form of a digital watermark. When illegally copied contents are seized, the embedded information is extracted to identify the person (that is, the purchaser) who produced the illegal copy.

Brief Summary Text (23):
The basic procedure for embedding purchaser's identification information is as follows: (1) The provider (contents provider) assigns a unique number to a contents purchaser. (2) The provider embeds the number of the contents purchaser into the contents in the form of a digital watermark. (3) When illegally-copied contents are found and seized, the provider or inspection division extracts the number from the contents to identify the purchaser. (4) The penalty is imposed on the purchaser for illegal copy or for lending the contents to a person who produced the illegal copy.

Brief Summary Text (38):
For example, with the illegal copy prevention technique described above, a number embedded in the illegally-copied contents cannot always be used as a proof that the illegally-copied contents were purchased by the purchaser corresponding to that number. That is, because the number was given by the provider one-sidedly, the purchaser may insist that the number found in the copy is not the one assigned to him or her.

Brief Summary Text (51):
To achieve the above objects, a method according to this invention is an embed-in-content information processing method for processing information embedded in a content using an electronic computer, the method comprising the steps of creating cryptographic information by encrypting specific data using a private key in accordance with a public key cipher system used by content-handling persons; and embedding the created cryptographic information into the content such that the

cryptographic information cannot be separated from the content without using a predetermined rule.

Brief Summary Text (55):
The cryptographic information embedded in the content may be a value dependent on the content into which the cryptographic information is to be embedded. For example, the value may be a digital signature generated by encrypting the hash value of the content. This value makes even clearer the correspondence between the information embedded in the illegal copy and the content-handling person of the content from which the illegal copy was created.

Brief Summary Text (56):
To achieve the above object, this invention is an embed-in-content information processing method for embedding information on k (k is an integer equal to or larger than 2) content-handling persons using an electronic computer, the method comprising the steps of embedding a digital signature into the content such that the digital signature cannot be separated from the content without using a predetermined rule, the digital signature being created by encrypting an n-bit hash value using a private key in accordance with a public key cipher system used by a first content-handling person, the n-bit hash value being obtained by evaluating the content with a first hash function; and sequentially repeating digital signature embedding for a second person to a k-th content-handling person, wherein, for an i-th content-handling person (i is an integer between 2 and k), the content into which the digital signatures of the first to an (i-1) content-handling persons are embedded is evaluated with a second hash function, wherein a resulting n/2-bit hash value is encrypted using the private key of the i-th content-handling person to generate the digital signature of the i-th content-handling person, and wherein the digital signature of the i-th content-handling person is embedded into the content in which the digital signatures from the first to the (i-1)th persons are already embedded such that the digital signature of the i-th content-handling person cannot be separated from the content without using a predetermined rule.

Brief Summary Text (59):
This invention is also an embed-in-content information processing method for embedding information on k (k is an integer equal to or larger than 2) content-handling persons using an electronic computer, the method comprising the steps of creating a digital signature of a first content-handling person by encrypting a hash value using a private key in accordance with a public key cipher system of the first content-handling person, the hash value being created by evaluating the content with a first hash function; sequentially repeating digital signature creation for a second person to a k-th content-handling persons to create the digital signatures of the content-handling persons; and embedding the digital signature of the k-th content-handling person into the content such that the digital signature cannot be separated from the content without using a predetermined rule, the digital signature being obtained by performing the digital signature creation for the k-th content-handling person, wherein, during the digital signature creation processing for an i-th content-handling person (i is an integer between 2 and k), a value dependent on the digital signature of the (i-1)th content-handling person is encrypted using the private key of the i-th content-handling person to generate the digital signature of the (i-1)th content-handling person. According to the embed-in-content information processing method, when the value determined by the value of the digital signature is n bits long, embedding only n-bit data into the content enables information for verifying k content-handling persons to be embedded into the content.

Brief Summary Text (68):
For example, this invention provides a content distribution system comprising a distribution system outputting a content to be distributed and a content receiving system receiving the distributed content, wherein the distribution system comprises encrypting means for encrypting a content to be distributed and wherein the

receiving system comprises decrypting means for decrypting a distributed content; signature creating means for creating cryptographic information by encrypting specific data using a private key in accordance with a public key cipher system used by a user of the receiving system; and signature embedding means for embedding the created cryptographic information into the content such that the cryptographic information cannot be separated from the content without using a predetermined rule.

Brief Summary Text (70):
This invention also provides a content distribution system wherein the encrypting means of the distribution system encrypts the content using the public key of the user of the receiving system and the decrypting means of the receiving system decrypts the content encrypted using the private key of the user of the distribution system.

Brief Summary Text (72):
In these content distribution systems, the signature creating means of the receiving system may use information containing a decrypted-content-dependent value as the specific data and may use a digital signature which the receiving system user has for the content as the cryptographic information, the digital signature being generated by encrypting the specific data using the private key in accordance with the public key cipher system used by the receiving system user.

Brief Summary Text (73):
This invention also provides a data processing system used to attach a signature to a content. This system comprises digital signature creating means for calculating a hash value by evaluating the content with a hash function and then encrypting the calculated hash value with a private key of a user of the data processing system in accordance with the public key cipher system used by the user to generate a digital signature; and digital watermark creating means for embedding the created digital signature into the content as a digital watermark.

Detailed Description Text (5):
The first embodiment explains an example of authentication of the relation between digital data and an individual/organization. More specifically, the embodiment explains an example of authentication of the relation between a content, one type of digital data, and a content purchaser, one type of individual/organization, in order to prevent the content from being copied illegally. However, it should be noted that the individual/organization need not always be a content purchaser. Depending upon the situation in which this embodiment is used, the first embodiment may be modified such that the individual/organization is a content copyright holder, a content vendor, a content wholesaler, or some other related person. In addition, in this embodiment and in the second and third embodiment that will be described later, the content is assumed to be image data. These embodiments may also be modified so that the content may contain other types of data, such as text data, drawing data, audio data, or video data.

Detailed Description Text (10):
As shown in the figure, the provider system 100 comprises a processing module 110 and a storage module 120. The processing module 110 comprises an input/output module 111 which performs input/output operations, a controlling module 112 which controls the components of the provider system 100, a signature extracting module 113 which extracts a digital signature from a content containing the digital signature, a signature verifying module 114 which verifies a digital signature, an encrypting module 115 which encrypts a content, and a sending/receiving module 116 which sends or receives data to or from each purchaser system 200. The storage module 120 stores contents 121 and verification keys 122. Note that the verification key 122 corresponds to the public key explained in Description of Related Art.

Detailed Description Text (11):
As shown in figure, the purchaser system 200 comprises a processing module 210 and a storage module 220. The processing module 210 comprises an input/output module 211 which performs input/output operations, a controlling module 212 which controls the components of the purchaser system 200, a sending/receiving module 213 which sends or receives data to or from the provider system 100, a decrypting module 214 which decrypts an encrypted content, a signature generating module 215 which generates a digital signature, a signature embedding module 216 which embeds a digital signature into a content, and a key generating module 217 which creates a signature key (private key) and a verification key (public key). The storage module 220 stores signature key 221 and signature-embedded contents 222. Note that the signature key 221 corresponds to the private key explained in Description of Related Art.

Detailed Description Text (19):
The controlling module 112 works with the input/output module 111 to accept the content to be distributed and stores it in the storage module 120. Then, as shown in FIG. 4, the controlling module 112 controls the encrypting module 115 to encrypt the stored content 121 with the use of the verification key 122 stored in the storage module 120 (step 401) and sends the encrypted content to the purchaser system 200 via the sending/receiving module 116 (step 402).

Detailed Description Text (20):
The purchaser system 200 performs the following operation when it receives the encrypted content.

Detailed Description Text (21):
As shown in FIG. 5, the controlling module 212 tells the decrypting module 214 to decrypt the encrypted content, received by the sending/receiving module 213, using the signature key stored in the storage module 220 (step 501) and then asks the signature generating module 215 to generate the digital signature of the decrypted content using the signature key stored in the storage module 220 (step 502).

Detailed Description Text (22):
To generate the digital signature, the signature generating module 215 calculates the 160-bit hash value of the decrypted content using a predetermined one-way hash function and then encrypts the resulting 160-bit hash value using the signature key stored in the storage module 220.

Detailed Description Text (25):
When the illegally-copied content in which the digital signature is embedded is seized, the provider system 100 performs the following to identify the purchaser who created the illegal copy.

Detailed Description Text (26):
That is, as shown in FIG. 6, the controlling module 112 of the provider system 100 works with the input/output module 111 to store the illegally-copied content in the storage module 120 and then tells the signature extracting module 113 to extract the digital signature from the illegally-copied content (step 601). Note that the storage module 120 of the provider system 100 contains the original content (with no digital signature embedded) of the illegally-copied content. This allows the signature extracting module 113 to find the difference between the original content and the illegally-copied content and therefore to extract the digital signature. If it is possible, the digital signature may be extracted according to the rule by which the digital signature was embedded into the content.

Detailed Description Text (27):
Next, the controlling module 112 tells the signature verifying module 114 to verify the digital signature (step 602). To do so, the signature verifying module 114 decrypts the extracted digital signature using the verification key 122 of a user

stored in the storage module 120 and compares the resulting value with the hash value obtained by evaluating the original content in the storage module 120 with the use of the same one-way hash function as that used by the purchaser system 200. If the rule used by the purchaser system 200 to embed the digital signature into the content is known only to the provider and if the digital signature may be removed from the content according to that rule, the content from which the digital signature is removed may be used instead of the original content.

Detailed Description Text (32):
Decryption and digital signature creation/embedding may also be carried out, not by the CPU 301 of the electronic computer shown in FIG. 3, but by a provider-supplied IC card which is protected against modification. In this case, upon receiving an encrypted content from the computer, the IC card which is connected to the computer returns the content in which digital signature is embedded.

Detailed Description Text (44):
Assume that the signature key and the verification key of the provider system 100 have already been generated and that the verification key of the provider system 100 has been distributed to each right-holder system. Also assume that each right-holder system 700 encrypts a content or various types of information using the verification key of the provider system 100 before sending them to the provider system 100 and that the provider system 100 decrypts received information using the signature key of the provider system 100. The encryption configuration and decryption configuration of information sent from each right-holder system 700 to the provider system 100 are omitted in FIG. 7, because they are the same as those of information sent from the provider system 100 to the right-holder system 700 or to the purchaser system 200.

Detailed Description Text (48):
The controlling module 112 works with the input/output module 111 to accept a distribution content, stores it in the storage module 120, asks the encrypting module 115 to encrypt the stored content 121 using the verification key 122, which is sent from the right-holder system 700 to which the content is to be sent and which is stored in the storage module 120, and sends the encrypted content to the right-holder system 700 via the sending/receiving module 116. When the content encrypted using the verification key of the provider system 100 is returned from the right-holder system 700, the provider system 100 decrypts it using the verification key of the provider system 100, encrypts the content using the verification key of the next right-holder system 700 to which the content is to be sent, and sends it to the next right-holder system 700. When sending the content, an instruction to use an abbreviated digital signature is sent to the right-holders system 700 other than the first one.

Detailed Description Text (49):
On the other hand, the right-holder system 700 which receives the encrypted content from the provider system 100 performs the following.

Detailed Description Text (50):
The controlling module 712 tells a decrypting module 714 to decrypt the encrypted content received via the sending/receiving module 713 using the signature key stored in the storage module 720, and tells a signature generating module 715 to generate a digital signature using the signature key of the decrypted content stored in the storage module 720.

Detailed Description Text (51):
To generate the digital signature, the 160-bit hash value of the decrypted content is calculated using a predetermined one-way hash function and the resulting 160-bit hash value is encrypted using the signature key stored in the storage module 720. If an instruction to use an abbreviated digital signature is attached to the received content, an 80-bit hash value is calculated and then encrypted using the

signature key stored in the storage module 720 to create a digital signature.

Detailed Description Text (60):
That is, in the third embodiment, the first right holder encrypts the content sent from the provider to generate a digital signature as in the second embodiment. However, unlike the second embodiment, the right-holder system 700 of the first right holder does not embed the digital signature in the content but returns the digital signature to the provider system 100. The provider system 100 receives the digital signature of the first right holder and sends it to the right-holder system 700 of the second right holder. The second right-holder system 700 encrypts the hash value of the first right holder's digital signature to generate a digital signature. This process is repeated for the subsequent right holders. The right-holder system 700 of the second and the subsequent right holders encrypts the hash value of the previous right holder's digital signature to generate his own digital signature.

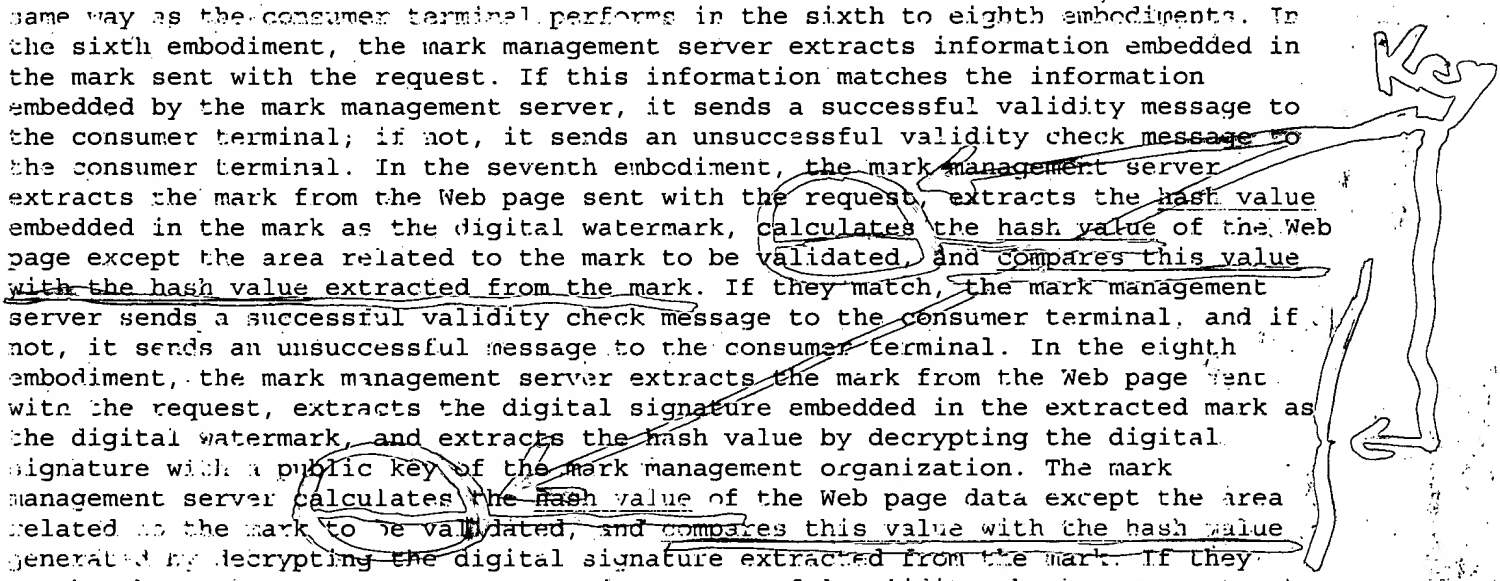
Detailed Description Text (63):
Digital signature embedding may also be carried out as follows. That is, the right-holder system 700 of the first right holder embeds a digital signature, created by encrypting the hash value of the content, into the content, and sends the content to the next right-holder system 700 via the provider system 100. The right-holder systems 700 of the second and the subsequent right holders each extract the previous right holder's digital signature from the content in which the digital signature is embedded, encrypts the hash value of the extracted digital signature to create the digital signature of his own, and embeds the created digital signature into the original content received from the provider system 100. Alternatively, each of the right-holder systems 700 replaces the previous right holder's digital signature, embedded in the content, with the digital signature of his own. The right-holder system 700 then sends the content, in which his digital signature is embedded, to the next right-holder system 700 via the provider system 100.

Detailed Description Text (196):
That is, as shown in FIG. 24, the terminal 1101 first extracts a mark 2407 from a Web page 2406 to check its validity (step 2401) and extracts a hash value 2408 embedded in the extracted mark 2407 as a digital watermark (step 2402). The terminal 1101 also calculates a hash value 2409 of the Web page data except the part related to the mark whose validity is to be checked (step 2403) and compares the calculated hash value 2409 with the hash value 2408 extracted from the mark (step 2404). If they match, the terminal 1101 displays a message stating that the mark was validated on the display unit 1102; if they do not match, the terminal 1101 displays a message stating that the mark was not validated on the display unit 1102 (step 2405).

Key

Detailed Description Text (212):
That is, as shown in FIG. 29, the terminal 1800a first gets a public key 2910 of the mark management organization 1121 from the public key DB 1801. Then, the terminal 1800a extracts a mark 2908 from a Web page 2907 to check its validity (step 2901), extracts a digital signature 2909 embedded in the extracted mark 2908 as a digital watermark (step 2902), and decrypts the extracted digital signature using the public key 2910 of the mark management organization 1121 to get a hash value 2911 (step 2903). The terminal 1800a also calculates a hash value 2912 of the Web page data except the part related to the mark 2908 whose validity is to be checked (step 2904), and compares the calculated hash value 2912 with the hash value 2911 generated by decrypting the digital signature extracted from the mark 2908 (step 2905). If they match, the terminal 1800a displays a message on the display unit 1102 stating that the mark was validated; if they do not match, the terminal 1800a displays a message staging that the mark was not validated (step 2906).

Detailed Description Text (219):
That is, in the sixth embodiment, the consumer terminal extracts the mark to be validated from the Web page, and sends the extracted mark and a validity check request to the mark management server. In the seventh and eighth embodiments, the consumer terminal sends Web page data containing the mark and the validity check request to the mark management server. On the display unit of the consumer terminal there is displayed a successful or an unsuccessful validity check message sent back from the mark management server. On the other hand, upon receiving a validity check request, the mark management server performs the validity check on the mark in the same way as the consumer terminal performs in the sixth to eighth embodiments. In the sixth embodiment, the mark management server extracts information embedded in the mark sent with the request. If this information matches the information embedded by the mark management server, it sends a successful validity message to the consumer terminal; if not, it sends an unsuccessful validity check message to the consumer terminal. In the seventh embodiment, the mark management server extracts the mark from the Web page sent with the request, extracts the hash value embedded in the mark as the digital watermark, calculates the hash value of the Web page except the area related to the mark to be validated, and compares this value with the hash value extracted from the mark. If they match, the mark management server sends a successful validity check message to the consumer terminal, and if not, it sends an unsuccessful message to the consumer terminal. In the eighth embodiment, the mark management server extracts the mark from the Web page sent with the request, extracts the digital signature embedded in the extracted mark as the digital watermark, and extracts the hash value by decrypting the digital signature with a public key of the mark management organization. The mark management server calculates the hash value of the Web page data except the area related to the mark to be validated, and compares this value with the hash value generated by decrypting the digital signature extracted from the mark. If they match, the mark management server sends a successful validity check message to the consumer terminal, and if not, it sends an unsuccessful message to the consumer terminal.



US Reference Agent Number (7)
[illegible]

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

☐ Generate Collection Print

L2: Entry 1 of 3 File: USPT Jul 8, 2003

US-PAT-NO: 6591250 ✓
DOCUMENT-IDENTIFIER: US 6591250 B1

TITLE: System and method for managing virtual property

DATE-ISSUED: July 8, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Johnson; Michael T.	Derry	NH		
Moromisato; George P.	Cambridge	MA		

US-CL-CURRENT: 705/51; 380/30, 705/3, 713/176

ABSTRACT:

A system and method for managing virtual property is disclosed. In the system, virtual items are each represented by one of [redacted] digital objects and are managed by one or more computer systems functioning as an owner, broker, authenticator and provider.

43 Claims, 14 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 14

Previous Doc Next Doc Go to Doc#

not same subj. matter 4

L2: Entry 2 of 3 File: USPT Oct 10, 2000

US-PAT-NO: 6131162
DOCUMENT-IDENTIFIER: US 6131162 A

TITLE: Digital data authentication method

DATE-ISSUED: October 10, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Yoshiura; Hiroshi	Kawasaki			JP
Takaragi; Kazuo	Ebina			JP
Sasaki; Ryoichi	Fujisawa			JP
Susaki; Seiichi	Yokohama			JP
Toyoshima; Hisashi	Hachioji			JP
Saito; Tsukasa	Tokyo			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Hitachi Ltd.	Tokyo			JP	03

APPL-NO: 09/ 090419 [PALM]
DATE FILED: June 4, 1998

PARENT-CASE:
CROSS REFERENCE TO RELATED APPLICATIONS This application is related to application Ser. No. 09/385,638, filed Aug. 27, 1999, entitled "Method of Generating Authentication Enabled Electronic Data", by Y. Nagai et al; and application Ser. No. 09/371,526, filed Aug. 10, 1999, entitled "Method of Appending Information to Image and Method of Extracting Information from Image", by H. Yoshiura et al.

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	9-148061	June 5, 1997
JP	9-348860	December 18, 1997

INT-CL: [07] H04 L 9/32, H04 L 9/28, H04 L 9/30

US-CL-ISSUED: 713/176; 713/170, 713/181, 705/57, 380/28, 380/30
US-CL-CURRENT: 713/176; 380/28, 380/30, 705/57, 713/170, 713/181

FIELD-OF-SEARCH: 380/30, 380/28, 380/202, 380/279, 380/283, 705/51-58, 713/150, 713/155, 713/162, 713/168, 713/170, 713/176, 713/180, 713/181

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL | Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5530759	June 1996	Braudaway et al.	380/54
☐	5872848	February 1999	Romney et al.	380/25
☐	5892904	April 1999	Atkinson et al.	395/187.01
☐	5898779	April 1999	Squilla et al.	380/23
☐	5960081	September 1999	Vynne et al.	380/10

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0855829	July 1989	EP	
0590884	April 1994	EP	
0705025	April 1996	EP	
0854633	July 1998	EP	
0859503	August 1998	EP	
53-148918	December 1978	JP	
6431198	February 1989	JP	

OTHER PUBLICATIONS

F. Rouaix, "A Web Navigator with Applets in Caml", 1996, Published by Elsevier Science B.V., Computer Networks and ISDN Systems 28, pp. 1365-1371.
S. Anderson, et al, "Sessioneer: Flexible Session Level Authentication with off the shelf servers and clients", 1995 Elsevier Science B.V., Computer Networks and ISDN Systems 27, pp. 1047-1053.
W. Bender, "Techniques for Data Hiding", IBM Systems Journal, vol. 35, No. 3 & 4, 1996, pp. 313-330.
N. Komatsu, et al, A Proposal on Digital Watermark in Document Image Communication and its Application to Realizing a Signature, Electronics and Communications in Japan 73(1990) May, No. 5, Part I, New York, US, pp. 22-33.
B. Schneier, Applied Cryptography 1996, John Wiley & Sons, US New York, pp. 39-41.
Sasaki, et al, Security Technology for Open Networks, Hitachi Review, JP, Hitachi, Ltd., Tokyo, vol. 46, No. 4, pp. 197-202.
M. Schneider et al, A Robust Content Based Digital Signature for Image Authentication, Proceedings of the International Conference on Image Processing, US, New York, IEEE, pp. 227-230.
W. Bender, Techniques for Data Hiding, IBM Systems Journal, vol. 35, No. 3 & 4, 1996, pp. 313-336.
Eiji Okamoto, Ango Riron Nyumon (Introduction to Cryptography), Kyoritsu Shuppan Co., Ltd., 1993, pp. 133-137.
Bruce Schneier, Applied Cryptography, 2.sup.nd Ed., John Wilsy & Sons, Inc., 1996, pp. 39-41.
Nikkei Electronics., No. 683, 1997, pp. 99-107.
Opendesign., Apr., 1996, pp. 4-22.
Opendesign., Apr. 1996, pp. 40-78.
Jyohoshori (Information Processing), Jyohoshori Gakkai (Information

Processing Society of Japan), vol. 38, No. 9, 1997, pp. 752-810.

ART-UNIT: 277

PRIMARY-EXAMINER: Swann; Tod R.

ASSISTANT-EXAMINER: Darrow; Justin T.

ATTY-AGENT-FIRM: Antonelli, Terry, Stout & Kraus, LLP

ABSTRACT:

This invention provides a method for identifying a purchaser who purchased content from which an illegal copy was produced. A provider system encrypts a content purchased by the purchaser using a public key of a purchaser system and sends the encrypted content to the purchaser system. The purchaser system creates a digital signature of the content with the use of a private key of its own and embeds the created digital signature into the received content. When an illegal copy is found, the provider system verifies the digital signature, embedded in the illegal copy as a digital watermark, to identify the purchaser who purchased the content from which the illegal copy was produced.

63 Claims, 29 Drawing figures

Previous Doc Next Doc Go to Doc#

cited

L2: Entry 3 of 3 File: USPT Feb 3, 1998

US-PAT-NO: 5715403
DOCUMENT-IDENTIFIER: US 5715403 A

TITLE: System for controlling the distribution and use of digital works having attached usage rights where the usage rights are defined by a usage rights grammar

DATE-ISSUED: February 3, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Stefik; Mark J.	Woodside	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Xerox Corporation	Stamford	CT			02

APPL-NO: 08/ 344041 [PALM]
DATE FILED: November 23, 1994

INT-CL: [06] G06 F 1/14, G06 F 13/372

US-CL-ISSUED: 395/244; 395/188.01, 395/800, 380/23
US-CL-CURRENT: 705/44; 705/54, 705/57, 709/229, 713/202

FIELD-OF-SEARCH: 395/800, 395/600, 395/700, 395/775, 395/650, 395/182.13, 395/608, 395/183.14, 395/201, 395/569, 395/825, 395/712, 395/187.01, 395/188.01, 395/244, 395/217, 380/4, 380/15, 380/18, 380/20, 380/25, 380/24, 380/23, 380/30, 364/DIG.1, 364/DIG.2, 364/41R, 340/825.33, 340/825.34, 348/3, 455/4.1, 455/5.1, 455/26.1

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	3790700	February 1974	Callais et al.	348/3
☐	4529870	July 1985	Chaum	235/380
☐	4658093	April 1987	Hellman	380/25
☐	4891838	January 1990	Faber	380/25
☐	4924378	May 1990	Hershey et al.	364/200

☐	4932054	June 1990	Chou et al.	380/4
☐	4937863	June 1990	Robert et al.	380/4
☐	4953209	August 1990	Ryder, Sr. et al.	380/23
☐	4961142	October 1990	Elliott et al.	364/408
☐	4977594	December 1990	Shear	380/4
☐	5010571	April 1991	Katznelson	380/4
☐	5014234	May 1991	Edwards, Jr.	364/900
☐	5023907	June 1991	Johnson et al.	380/4
☐	5047928	September 1991	Wiedemer	364/406
☐	5050213	September 1991	Shear	380/25
☐	5058164	October 1991	Elmer et al.	380/50
☐	5103476	April 1992	Waite et al.	380/4
☐	5113519	May 1992	Johnson et al.	395/600
☐	5138712	August 1992	Corbin	395/700
☐	5146499	September 1992	Geffrotin	380/23
☐	5159182	October 1992	Eisele	235/492
☐	5191193	March 1993	Le Roux	235/379
☐	5204897	April 1993	Wyman	380/4
☐	5247575	September 1993	Sprague et al.	380/9
☐	5255106	October 1993	Castro	380/18
☐	5260999	November 1993	Wyman	380/4
☐	5291596	March 1994	Mita	395/608
☐	5339091	August 1994	Yamazaki et al.	345/104

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0332707	September 1989	EP	
2236604	April 1991	GB	
WO9220022	November 1992	WO	
9301550	January 1993	WO	

OTHER PUBLICATIONS

Press Release From Electronic Publishing Resources, Inc. (EPR) entitled "National Semiconductor and EPR Partner for Information Metering/Data Security Cards", dated Mar. 4, 1994.
Weber, R., "Digital Rights Management Technology", Oct. 1995.
European Search Report for Corresponding European Application 95308417.5.
U. Flasche et al., Decentralized Processing of Documents, Comput. & Graphics, vol. 10, No. 2, 1986, pp. 119-131.
R. Mori et al., Superdistribution: The Concept and the Architecture, The Transactions of the IEICE, vol. E 73, No. 7, 1990, Tokyo, JP, pp. 1133-1146.

Weber, R., "Metering Technologies For Digital Intellectual Property," A Report to the International Federation of Reproduction Rights Organizations, Oct. 1994, pp. 1-29.
Clark, P.C. and Hoffman, L.J., "Bits: A Smartcard Protected Operating System," Communications of the ACM, Nov. 1994, vol. 37, No. 11, pp. 66-70, and 94.
Ross, P.E., "Data guard", Forbes, Jun. 6, 1994, p. 101.
Saigh, W.K., "Knowledge is Sacred," Video Pocket/Page Reader Systems, Ltd., 1992.
Kahn, R.E., "Deposit, Registration And Recordation In An Electronic Copyright Management System," Corporation for National Research Initiatives, Virginia, Aug. 1992, pp. 1-19.
Hilts, P., Mutter, J., and Taylor, S., "Books While U Wait," Publishers Weekly, Jan. 3, 1994, pp. 48-50.
Strattner, A., `"Cash register on a chip" may revolutionize software pricing and distribution; Wave Systems Corp.,` Computer Shopper. Copyright, Apr. 1994, vol. 14; No. 4; p. 62; ISSN 0886-0556.
O'Conner, M.A., "New distribution option for electronic publishers; iOpener data encryption and metering system for CD-ROM use; Column," CD-ROM Professional, Copyright, Mar. 1994, vol. 7; No. 2; p. 134; ISSN: 1049-0833.
Willett, S., `"Metered PCs: Is your system watching you?"; Wave Systems beta tests new technology,` InfoWorld, Copyright, May 2, 1994, p. 84.
Linn, R.J., "Copyright and Information Services in the Context of the National Research and Education Network.sup.1," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 9-20.
erritt, Jr., H.H., "Permissions Headers and Contract Law," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 27-48.
Upthegrove, L., and Roberts, R., "Intellectual Property Header Descriptors: A Dynamic Approach," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 63-66.
Sirbu, M.A., "Internet Billing Service Design and Prototype Implementation," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 67-80.
Simmel, S.S., and Godard, I., "Metering and Licensing of Resources: Kala's General Purpose Approach," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 81-110.
Kahn, R.E., "Deposit, Registration and Recordation in an Electronic Copyright Management System," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 111-120.
Tygar, J.D., and Bennet, Y., "Dyad: A System for Using Physically Secure Coprocessors," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 121-152.
Griswold, G.N., "A Method for Protecting Copyright on Networks," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 169-178.
Nelson, T.H., "A Publishing and Royalty Model for Networked Documents," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 257-259.

ART-UNIT: 232

PRIMARY-EXAMINER: Pan; Daniel H.

ATTY-AGENT-FIRM: Domingo; Richard B.

ABSTRACT:

A system for controlling use and distribution of digital works. The present invention allows the owner of a digital work to attach usage rights to their work. The usage rights define how the individual digital work may be used and distributed. Instances of usage rights are defined using a flexible and extensible usage rights grammar. Conceptually, a right in the usage rights grammar is a label associated with a predetermined behavior and conditions to exercising the right.

The behavior of a usage right is embodied in a predetermined set of usage transactions steps. The usage transaction steps further check all conditions which must be satisfied before the right may be exercised. These usage transaction steps define a protocol for requesting the exercise of a right and the carrying out of a right.

28 Claims, 20 Drawing figures

Previous Doc Next Doc Go to Doc#

L7: Entry 1 of 1 File: USPT Apr 27, 1999

DOCUMENT-IDENTIFIER: US 5898779 A
TITLE: Photograhic system with selected area image authentication

Application Filing Date (1):
19970414

Detailed Description Text (15):
The authentication process is depicted in FIG. 6. Since the decryption key (public key) of the camera is publicly available through a directory or a similar means, any user who wants to authenticate the image can use that key to decrypt the appended signature. The first step is to separate the digital signature from the digital image (separation step 82) and the unencrypted header information including the photographer's information. The decrypted signature will include a hashed value of the image information along with the "photographer's information". At this point, if desired, the "photographer's information" can be matched against the unencrypted "photographer's information" that is also included as part of the original image file. The next step in the process is to use the unencrypted header information to determine the regions of the image (identification step 84) that were selected for authentication at the time of picture taking and to select those pixels from the image that needs to be authenticated. The selected pixel values are then hashed in the same manner that was used in the camera (new hash step 86). Meanwhile, the digital signal is decrypted using the public key (decryption step 88) to obtain a decrypted hash value. If the new hashed value is identical to the decrypted hash value (compare step 90), the image is authentic and no tampering has been done to the image since it has been captured by the camera. This is because it is computationally infeasible to generate an encrypted data file that would decrypt into a desired hash value without knowing the private key.

Detailed Description Text (18):
The authentication process can also be employed in a digital device using the FlashPix.TM. architecture and image file format (see FlashPix Format Specification, Version 1.0 (1996), available at the Eastman Kodak Co. Web site at www.kodak.com/go/flashpix). A FlashPix.TM. file contains the complete image plus a hierarchy of several lower-resolution copies within the same file. Images at each resolution also are divided into rectangular tiles (e.g., squares), which enable the application to minimize the amount of image data processed to access, display or print a portion of the scene content. One advantage of the FlashPix.TM. format is that each tile has its own autonomy, and can be singled out for processing separate from the other tiles. In order to implement selected area image authentication on a FlashPix.TM. file, the tile pattern 12 as shown in FIG. 1B may be established such that its grid pattern corresponds to the FlashPix.TM. tile pattern and the corresponding FlashPix.TM. tiles are activated during the authentication process. If custom tile patterns or preset templates are chosen as shown in FIG. 3, the custom pattern is expanded as necessary by the logic control unit 34 to include an integral number of FlashPix.TM. tiles. For example, as shown in FIG. 8, if a preset template 92 covers a partial area of some tiles 94 within a FlashPix.TM. grid pattern 96, the actual pattern processed by the signal processing section 26 will be expanded by the logic control unit 34 to cover a plurality of

whole tiles as shown by the expanded template 98. While the FlashPix.TM. format contains a hierarchy of lower-resolution copies of the image, and authentication could be performed on any or all of the copies, the authentication process would typically be performed on a selected area of the complete image.

CLAIMS:

15. An encryption system as claimed in claim 13 wherein the system further includes means for generating photographer's information including at least one of the time of the day, one or more exposure settings, the name of the photographer, information about the scene and its content, and other information required by the application.

Previous Doc Next Doc Go to Doc#

reviewed

Forward Ref

L4	l3 and @ad<=20001113 and (compar$ with hash$ with (number$ or value)) and (encrypt$ with content) and ((updat$ or cop$) same content)	4	L4
L3	('6131162'|'6591250'|'5715403')[URPN]	114	L3
L2	L1 or 5715403.pn. or 6591250.pn.	3	L2
L1	6131162.pn.	1	L1

END OF SEARCH HISTORY

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

End of Result Set

☐ Generate Collection Print

L7: Entry 1 of 1 File: USPT Apr 27, 1999

US-PAT-NO: 5898779
DOCUMENT-IDENTIFIER: US 5898779 A

TITLE: Photograhic system with selected area image authentication

DATE-ISSUED: April 27, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Squilla; John R.	Rochester	NY		
Moghadam; Omid A.	Rochester	NY		
Rabbani; Majid	Pittsford	NY		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Eastman Kodak Company	Rochester	NY			02

APPL-NO: 08/ 837186 [PALM]
DATE FILED: April 14, 1997

INT-CL: [06] H04 K 1/00

US-CL-ISSUED: 380/23; 380/4
US-CL-CURRENT: 713/176; 380/200

FIELD-OF-SEARCH: 380/23, 380/7, 380/4, 380/5, 380/51

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5499294	March 1996	Friedman	380/10
☐	5799082	August 1998	Murphy et al.	380/7
☐	5799083	August 1998	Brothers et al.	380/23

OTHER PUBLICATIONS

Handbook of Applied Cryptography, Menezes, et al. pp. 321-661, Dec. 1997.
"A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,"

Elgamal, IEEE Transactions on Information Theory, V IT31, N4, Jul. 1985.
"A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Rivest, et al. Communications of the ACM V21, N2, Feb. 1978.
"One-Way Hash Functions: Using cryptographic algorithms for hashing" by Bruce Schneier. Dr. Dobbs's Journal, Sep. 1991, pp. 148-151.
"New Directions in Cryptography" by Whitfield Diffie and Martin E. Hellman. IEEE Transactions on Information Theory, vol. IT-22, No. 6, Nov. 1976, pp. 644-654.

ART-UNIT: 276

PRIMARY-EXAMINER: Cain; David.

ATTY-AGENT-FIRM: Woods; David M.

ABSTRACT:

A public key encryption system for authenticating an image includes a digital camera having embedded therein a private key unique to the digital camera. A known public key uniquely based upon the private key is used to decrypt digital data encrypted with the private key to establish authenticity of the image. The encryption system further comprises means for generating one or more patterns each composed of at least one individual area that is visible together with the image of the object, means for designating at least one individual area as an active area of the image suitable for authentication and for generating location data identifying the active area, and means for calculating image hash from image data of the active area of the image using a predetermined hash algorithm. The image hash is then encrypted with the embedded private key, thereby producing a digital signature uniquely associated with the active area of the image, and the image data, the digital signature, and the location data of said active area are stored in a digital record. By confining encryption to this selected region of interest, power requirements for subsequent hashing and encryption are reduced, which is an advantage for portable devices such as a digital camera.

36 Claims, 11 Drawing figures

Previous Doc Next Doc Go to Doc#

L7: Entry 1 of 1 File: USPT Apr 27, 1999

DOCUMENT-IDENTIFIER: US 5898779 A
TITLE: Photograhic system with selected area image authentication

Application Filing Date (1):
19970414

Detailed Description Text (15):
The authentication process is depicted in FIG. 6. Since the decryption key (public key) of the camera is publicly available through a directory or a similar means, any user who wants to authenticate the image can use that key to decrypt the appended signature. The first step is to separate the digital signature from the digital image (separation step 82) and the unencrypted header information including the photographer's information. The decrypted signature will include a hashed value of the image information along with the "photographer's information". At this point, if desired, the "photographer's information" can be matched against the unencrypted "photographer's information" that is also included as part of the original image file. The next step in the process is to use the unencrypted header information to determine the regions of the image (identification step 84) that were selected for authentication at the time of picture taking and to select those pixels from the image that needs to be authenticated. The selected pixel values are then hashed in the same manner that was used in the camera (new hash step 86). Meanwhile, the digital signal is decrypted using the public key (decryption step 88) to obtain a decrypted hash value. If the new hashed value is identical to the decrypted hash value (compare step 90), the image is authentic and no tampering has been done to the image since it has been captured by the camera. This is because it is computationally infeasible to generate an encrypted data file that would decrypt into a desired hash value without knowing the private key.

Detailed Description Text (18):
The authentication process can also be employed in a digital device using the FlashPix.TM. architecture and image file format (see FlashPix Format Specification, Version 1.0 (1996), available at the Eastman Kodak Co. Web site at www.kodak.com/go/flashpix). A FlashPix.TM. file contains the complete image plus a hierarchy of several lower-resolution copies within the same file. Images at each resolution also are divided into rectangular tiles (e.g., squares), which enable the application to minimize the amount of image data processed to access, display or print a portion of the scene content. One advantage of the FlashPix.TM. format is that each tile has its own autonomy, and can be singled out for processing separate from the other tiles. In order to implement selected area image authentication on a FlashPix.TM. file, the tile pattern 12 as shown in FIG. 1B may be established such that its grid pattern corresponds to the FlashPix.TM. tile pattern and the corresponding FlashPix.TM. tiles are activated during the authentication process. If custom tile patterns or preset templates are chosen as shown in FIG. 3, the custom pattern is expanded as necessary by the logic control unit 34 to include an integral number of FlashPix.TM. tiles. For example, as shown in FIG. 8, if a preset template 92 covers a partial area of some tiles 94 within a FlashPix.TM. grid pattern 96, the actual pattern processed by the signal processing section 26 will be expanded by the logic control unit 34 to cover a plurality of

L4: Entry 1 of 4 File: USPT Feb 22, 2005

US-PAT-NO: 6859790
DOCUMENT-IDENTIFIER: US 6859790 B1

TITLE: Data distribution system and method thereof, data processing device, data control device, and machine-readable recording medium recording distribution data

DATE-ISSUED: February 22, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Nonaka; Akira	Kanagawa			JP
Ezaki; Tadashi	Tokyo			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Sony Corporation	Tokyo			JP	03

APPL-NO: 09/ 691410 [PALM]
DATE FILED: October 18, 2000 ✓

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	11-298921	October 20, 1999 ✓

INT-CL: [07] G06T01760

US-CL-ISSUED: 705/51; 705/1, 705/51, 705/55, 705/57, 380/3, 380/4, 380/255, 707/9, 707/65, 713/189, 713/193, 713/194
US-CL-CURRENT: 705/51; 380/255, 705/1, 705/55, 705/57, 705/65, 707/9, 713/189, 713/193, 713/194

FIELD-OF-SEARCH: 705/51, 705/1, 705/55, 705/57, 380/3, 380/4, 380/255, 707/65, 707/9, 713/189, 713/193, 713/194

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5715403	February 1998	Stefik	705/44
☐	5825883	October 1998	Archibald et al.	705/53

☐	6016509	January 2000	Dedrick	709/224
☐	6233684	May 2001	Stefik et al.	713/176
☐	6289455	September 2001	Kocher et al.	713/194
☐	6341273	January 2002	Briscoe	705/41

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
2002230428	August 2002	JP	

OTHER PUBLICATIONS

http://www.vector-networks.com/pcduo-enterprise/datasheets/ Software_Metering.pdf.

ART-UNIT: 3621

PRIMARY-EXAMINER: Trammell; James P.

ASSISTANT-EXAMINER: Winter; J

ATTY-AGENT-FIRM: Frommer Lawrence & Haug LLP Frommer; William S.

ABSTRACT:

A contents provider stores contents data in a container in a format which can only be decoded with a key distributed from an EMD service center, and transmits the container to a service provider. The service provider adds pricing information and the like and distributes this to a user home network. The user home network pays charges to the EMD service center based on the pricing information, receives the key, and decodes the contents data. Information regarding the number of times which copying is permitted is contained in the secure container, and the number of times permitted is increased each time charges are paid, thereby enabling copying to other media and the like. It is impossible to make copies from a container simply copied, or in cases where in the number of permitted times of copies has been used up. Thus, contents data can be distributed in a format wherein copying of contents data can be controlled including the number of copies made.

36 Claims, 34 Drawing figures

Previous Doc Next Doc Go to Doc#

L4: Entry 2 of 4 File: USPT Aug 24, 2004

US-PAT-NO: 6782190 ?
DOCUMENT-IDENTIFIER: US 6782190 B1

TITLE: Copy protection apparatus and method

DATE-ISSUED: August 24, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Morito; Hajime	Yokohama			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Hitachi, Ltd.	Tokyo			JP	03

APPL-NO: 09/ 388770 [PALM] ✓
DATE FILED: September 2, 1999

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
EP	98307028	September 2, 1998

INT-CL: [07] H04 N 5/91

US-CL-ISSUED: 386/94; 360/60, 380/201
US-CL-CURRENT: 386/94; 360/60, 380/201

FIELD-OF-SEARCH: 386/94, 380/201, 380/203, 380/28, 380/30, 360/60, 705/57-58, 705/51, 705/54, 713/193, 358/403

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5323244	June 1994	Yamaguchi et al.	386/94
☐	5661800	August 1997	Nakashima et al.	
☐	5761301	June 1998	Oshima et al.	
☐	5987607	November 1999	Tsumura	380/203
☐	6131162	October 2000	Yoshiura et al.	380/28

☐	6282654	August 2001	Ikeda et al.	380/203
☐	6289102	September 2001	Ueda et al.	380/201
☐	6295139	September 2001	Yamauchi et al.	358/403
☐	6301430	October 2001	Oguro et al.	386/94

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
553 545	August 1993	EP	
809 244	November 1997	EP	

ART-UNIT: 2615

PRIMARY-EXAMINER: Tran; Thai

ASSISTANT-EXAMINER: Onuaku; Christopher

ATTY-AGENT-FIRM: Mattingly, Stanger & Malur, P.C.

ABSTRACT:

An apparatus and method of copy protection for use in digital data recorders such as DVD-RAM recorders (30), which includes using DVD disks (1) with unique serial numbers stored in a read only part (2) of the disk for recording data. The serial number of each disk together with other copy control information is digitally signed. The digital signature is verified at the DVD player/recorder (13, 30) to check whether the disk being played is an original disk or an authorized copy. If not, play back and recording of the data on the disk is prevented. The use of copy control information also allows the implementation of a copy generation management system.

23 Claims, 17 Drawing figures

Previous Doc Next Doc Go to Doc#

L4: Entry 3 of 4 File: USPT Jul 29, 2003

US-PAT-NO: 6601046
DOCUMENT-IDENTIFIER: US 6601046 B1

TITLE: Usage dependent ticket to protect copy-protected material

DATE-ISSUED: July 29, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Epstein; Michael A.	Spring Valley	NY		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Koninklijke Philips Electronics N.V.	Eindhoven			NL	03

APPL-NO: 09/ 454350 [PALM]
DATE FILED: December 3, 1999

PARENT-CASE:
This application claims the benefit of U.S. Provisional Application No. 60/126,167 filed Mar. 25, 1999,

INT-CL: [07] G06 F 12/14

US-CL-ISSUED: 705/57; 705/52, 360/55, 713/17C
US-CL-CURRENT: 705/57; 360/55, 705/52

FIELD-OF-SEARCH: 705/57, 705/52, 360/55, 713/176

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4977594	December 1990	Shear	705/52
☐	5247575	September 1993	Sprague et al.	379/55.1
☐	5715403	February 1998	Stefik	705/44
☐	5887060	March 1999	Ronning	705/27
☐	5982891	November 1999	Ginter et al.	705/26
☐	6049789	April 2000	Frison et al.	705/30

☐	6236971	May 2001	Stefik et al.	705/1

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
2811839	November 2000	FR	

OTHER PUBLICATIONS

IBM TDB NN9509345, Methods for thwarting corrupt implemenataion of data encryption, Sep. 1995.

ART-UNIT: 3621

PRIMARY-EXAMINER: Hayes; John W.

ASSISTANT-EXAMINER: Winter; John M

ATTY-AGENT-FIRM: Goodman; Edward W.

ABSTRACT:

A usage-limit is associated with each copy of copy-protected material. A conforming playback device determines how much usage has been made of the copy, and only plays the copy-protected material if the usage is within the associated usage-limit of the copy. In a preferred embodiment of this invention, the providing source of the copy contains a total-usage-measure that is allocated among each of the provided copies of the copy-protected material, thereby allowing for more than one copy of the copy-protected material to be produced, or "checked-out" from the providing source. When a copy of the copy-protected material is subsequently returned, or "checked-in" to the providing source, the usage allocation associated with this copy is returned to the total-usage-value. In this manner, if a particular copy of the copy-protected material is lost, damaged, or misplaced, the loss of value to the purchaser is merely a reduction in the available total-usage. In a preferred embodiment, the parameters associated with the usage-limit are communicated via the copy of the material in a secure manner, so that an illicit provider cannot alter these parameters. Similarly, in a preferred embodiment, the parameters associated with the usage-limit are securely bound to the copy-protected material, so that an illicit provider cannot substitute illicit material for the copied material. Other security measures, such as an encryption of the copy-protected material, watermarking, ticketing, and the like, are also compatible with these aforementioned techniques, and are included in a preferred embodiment of this invention.

10 Claims, 3 Drawing figures

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

End of Result Set

☐ Generate Collection Print

L4: Entry 4 of 4 File: USPT Dec 24, 2002

US-PAT-NO: 6499105
DOCUMENT-IDENTIFIER: US 6499105 B1

TITLE: Digital data authentication method

DATE-ISSUED: December 24, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Yoshiura; Hiroshi	Kawasaki			JP
Takaragi; Kazuo	Ebina			JP
Sasaki; Ryoichi	Fujisawa			JP
Susaki; Seiichi	Yokohama			JP
Toyoshima; Hisashi	Hachioji			JP
Saito; Tsukasa	Tokyo			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Hitachi, Ltd.	Tokyo			JP	03

APPL-NO: 09/ 621697 [PALM]
DATE FILED: July 21, 2000

PARENT-CASE:
This application is a continuation of U.S. patent application Ser. No. 09/090,419, filed Jun. 4, 1998, now U.S. Pat. No. 6,131,162 A.

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	9-148061	June 5, 1997
JP	9-348860	December 18, 1997

INT-CL: [07] H04 L 9/32, H04 L 9/30

US-CL-ISSUED: 713/176; 713/170, 713/181, 705/51, 380/202
US-CL-CURRENT: 713/176; 380/202, 705/51, 713/170, 713/181

FIELD-OF-SEARCH: 713/150, 713/155, 713/168, 713/170, 713/176, 713/181, 713/201, 380/28, 380/30, 380/202, 705/51, 705/52, 705/53, 705/54, 705/55, 705/56, 705/57, 705/58

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL | Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5530759	June 1996	Braudaway et al.	380/54
☐	5825892	October 1998	Braudaway et al.	380/51
☐	5872848	February 1999	Romney et al.	380/25
☐	5892904	April 1999	Atkinson et al.	713/201
☐	5898779	April 1999	Squilla et al.	380/23
☐	5960081	September 1999	Vynne et al.	380/10
☐	6131162	October 2000	Yoshiura et al.	713/176
☐	6201879	March 2001	Bender et al.	382/100
☐	6359985	March 2002	Koch et al.	380/54

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0590884	April 1994	EP	
0705025	April 1996	EP	
0854633	July 1998	EP	
0855829	July 1998	EP	
0859503	August 1998	EP	
53148918	December 1978	JP	
6431198	February 1989	JP	
6119225	April 1994	JP	

OTHER PUBLICATIONS

W. Bender, "Techniques for Data Hiding", IBM Systems Journal, vol. 35, No. 3 & 4, 1996, pp. 313-336.
E. Okamoto, Ango Riron Nyumon (Introduction to Cryptography), Kyoritsu Shuppan Co., Ltd., 1993, pp. 133-137.
B. Schneier, Applied Cryptography, 2.sup.nd Ed., John Wilsy & Sons, Inc., 1996, pp. 39-41.
Nikkei Electronics, N. 683, 1997, pp. 99-107.
Opendesign, Apr. 1996, pp. 4-22.
Opendesign, Apr. 1996, pp. 40-78.
Jyohoshori (Information Processing), Jyohoshori Gakk ai (Information Processing Society of Japan), vol. 38, No. 9, 1997, pp. 752-810.
N. Komatsu, et al, A Proposal on Digital Watermark in Document Image Communication and its Application to Realizing a Signature, Electronics and Communication in Japan 73(1990) May, No. 5, Part 1, New York, US, pp. 22-33.
B. Schneier, Applied Cryptography, 1996, John Wiley & Sons, US. New York, pp. 39-41.
Sasaki, et al, Security Technology for Open Networks, Hitachi Review, JP, Hitachi, Ltd., Tokyo vol. 46, No. 4, pp. 197-202.
M. Schneider et al, A Robust Content Based Digital Signature for Image Authentication, Proceedings of the International conference on Image Processing,

US, New Yori, IEEE, pp. 227-230.
F. Rouaix, "A Web Navigator with Applets in Caml", 1996, Published by Elsevier Science B.V., Computer Networks and ISDN System 28, pp. 1365-1371.
S. Anderson, et al, "Sessioner: Flexible Session Level Authentication with off the shelf servers and clients", 1995 Elsevier Science B.V., Computer Networks and ISDN Systems 27, pp. 1047-1053.

ART-UNIT: 2132

PRIMARY-EXAMINER: Darrow; Justin T.

ATTY-AGENT-FIRM: Antonelli, Terry, Stout & Kraus, LLP

ABSTRACT:

This invention provides a method for identifying a purchaser who purchased content from which an illegal copy was produced. A provider system encrypts purchased by the purchaser using a public key of a purchaser system and sends the encrypted content to the purchaser system. The purchaser system creates a digital signature of the content with the use of a private key of its own and embeds the created digital signature into the received content. When an illegal copy is found, the provider system verifies the digital signature, embedded in the illegal copy as a digital watermark, to identify the purchaser who purchased the content from which the illegal copy was produced.

60 Claims, 29 Drawing figures

Previous Doc Next Doc Go to Doc#